

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND the claims in accordance with the following:

1. (Currently Amended) A security management device including:
 a security detection unit to detect a security level of a user apparatus;
 a judging unit to judge whether the security level of the user apparatus reaches a predetermined security level; and
 an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, to restrict as a restriction range an access permission range on a network of the user apparatus to be within a predetermined range on a network, wherein
 the security management device sends a program to the user apparatus and causes the user apparatus to set the security setting of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level,
the security setting is a setting as to whether to respond to a specified command.
2. (Previously Presented) A security management device according to Claim 1, wherein the access control unit, in case the judging unit judges that the security level of the user apparatus reaches the predetermined level, sets a range wider than the restriction range as the access permission range of the user apparatus.
3. (Previously Presented) A security management device according to Claim 1, wherein the access control unit has a function of controlling a communication route of the user apparatus and, in case the judging unit judges that the security level of the user apparatus does not reach the predetermined level, as the restriction range controls a communication destination of the user apparatus to a security setting guide server management device.

4. (Previously Presented) A security management device according to Claim 3, wherein the security setting guide server management device controls updating the virus definition file of the user apparatus.

5. (Currently Amended) A method of managing computer security comprising:
detecting a security level of a user apparatus;
judging whether the security level of the user apparatus reaches a predetermined security level; [[and]]

in case of judging the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network of the user apparatus to be within a predetermined range on a network ;

sending a program to the user apparatus; and

causing the user apparatus to set ~~the~~ security setting of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level.

wherein the security setting is a setting as to whether to respond to a specified command.

6. (Previously Presented) A security management method according to Claim 5, wherein in case of judging the security level of the user apparatus reaches the predetermined level, setting a range wider than the restriction range as the access permission range of the user apparatus.

7. (Previously Presented) A security management method according to Claim 5, wherein in case of judging the security level of the user apparatus does not reach the predetermined level, the restricting of the access permission range of the user apparatus comprises changing a communication destination of the user apparatus to a security setting guide server management device on the network.

8. (Previously Presented) A security management method according to Claim 7, wherein the security setting guide server management device controls updating the virus definition file of the user apparatus.

9. (Currently Amended) A non-transitory recording medium recorded with a security management program for making a computer execute:

detecting a security level of a user apparatus;
judging whether the security level of the user apparatus reaches a predetermined security level;
in case of judging the security level of the user apparatus does not reach the predetermined security level, restricting an access permission range on a network of the user apparatus to be within a predetermined range on a network ;
sending a program to the user apparatus; and
causing the user apparatus to set the security setting of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level,
wherein the security setting is a setting as to whether to respond to a specified command.

10. (Previously Presented) A non-transitory recording medium recorded with a security management program according to Claim 9, wherein in case of judging the security level of the user apparatus reaches the predetermined security level, setting a range wider than the restriction range as the access permission range of the user apparatus.

11. (Previously Presented) A non-transitory recording medium recorded with a security management program according to Claim 9, wherein in case of judging the security level of the user apparatus does not reach the predetermined security level, the restricting of the access permission range of the user apparatus comprises changing a communication destination of the user apparatus to a security setting guide server management device on the network.

12. (Previously Presented) A non-transitory recording medium recorded with a security management program according to Claim 11, wherein the security setting guide server management device controls updating the virus definition file of the user apparatus.

13. (Currently Amended) A security management system comprising:
a security management device; and
an apparatus for a user,
wherein the security management device executes:
a detection unit to detect a security level of a user apparatus,
a judging unit to judge whether the security level of the user apparatus reaches a predetermined security level,

an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, to restrict an access permission range on a network of the user apparatus to be within a predetermined range on a network , and

a sending unit to send a program to the user apparatus and to cause the user apparatus to set the security setting of the user apparatus by executing the program, when the security level of the user apparatus does not reach the predetermined security level,

the security setting is a setting as to whether to respond to a specified command.

14. (Previously Presented) A security management system according to Claim 13, wherein the access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, connects the user apparatus to the security setting guide device.

15-18. (Cancelled)

19. (Previously Presented) The security management device according to Claim 1, wherein the user apparatus is established to afford the network.

20. (Previously Presented) The security management device according to claim 1, wherein the access control unit, in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, does not restrict the access permission range on the network of the user apparatus.

21. (Previously Presented) The security management method according to Claim 5, wherein the user apparatus is established to afford the network.

22. (Previously Presented) The security management method according to claim 5, wherein in the case when it is judged that the security level of the user apparatus has reached the predetermined security level, the access permission range on the network of the user apparatus is not restricted.

23. (Previously Presented) The security management system according to Claim 13, wherein the user apparatus is established to afford the network.

24. (Previously Presented) The security management system according to claim 13, wherein the access control unit of the security management system, in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, does not restrict the access permission range on the network of the user apparatus.

25-28. (Cancelled)

29. (Currently Amended) A security management device comprising:
a security detection unit to detect a security level of a user apparatus;
a judging unit to judge whether the security level of the user apparatus reaches a predetermined security level; and
an access control unit to restrict an access permission range on a network of the user apparatus within a first range on a network when the judging unit judges the security level of the user apparatus does not reach the predetermined security level, and to set the access permission range on the network to a second range that exceeds the first range when the judging unit judges the security level of the user apparatus reaches the predetermined security level, wherein

the security management device sends a program to the user apparatus and causes the user apparatus to set the security setting of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level,
the security setting is a setting as to whether to respond to a specified command.

30. (Previously Presented) The security management device according to claim 29, wherein the access control unit restricts the user apparatus to access and/or become accessible to apparatuses within the first range on the network including the security management device and an apparatus that provides the virus definition file to the user apparatus.